Talk Nerdy To Me

March 2022

Luck Is For Leprechauns! Make Sure Your Data Is Safe.

If your server suddenly crashed and ALL your data was erased, how long would it take before your business was back up and running as usual?

If you aren't sure, or if you think it would only be a short period of time, read on. Below are 3 common costly misunderstandings most business owners have about their data backup that give them a false sense of security:

Misunderstanding #1: Believing that tape backups are a reliable way to secure your data...Wrong! Tape backups have an average failure rate of 100% (no that's not a typo). What makes this even worse is that tape backups will APPEAR to be working, giving you a false sense of security.

Misunderstanding #2: Relying on an inexpensive, automated online backup provider to backup your company data. Tread carefully here and make sure that you've really done your homework on your chosen solution. Here are a few questions to ask of any offsite backup provider before you trust your company data with them:

1. Ask if you have the option to have your initial backup performed through a hard copy. With the amount of data on most company's servers, an initial backup performed over the web can take months to complete.

2. Make sure that database files can be stored and recovered easily. Many cheap online backup services only hold simple office or media files, while ignoring your most important database files or making those incredibly difficult to recover.

3. Demand daily status reports. Any reputable backup service will send you a daily e-mail to verify that everything is backed up. The more professional solutions will allow you to notify more than 1 person (like your IT) in addition to yourself.

Misunderstanding #3: Trusting their backup is automatically working without doing periodic test restores. We see this happen a lot - a business owner thinks their backups are working because they don't see any error messages or apparent problems. Then, when they need to restore a file (or the entire server), the discover the backups stopped working MONTHS ago and all that data is gone.

Contact us today to make sure you have the fastest, most reliable way to recover your data!

Microsoft Accounts Targeted By Russian-Themed Credential Harvesting

While legitimate concerns abound about the Russian-Ukrainian conflict spark a far-reaching cyberwarfare conflagration around the globe, small-time crooks are also ramping up their efforts amid the crisis. Phishing emails to Microsoft users warning of Moscow-led account hacking have started to make the rounds, looking to lift credentials and other personal details.

That's according to Malwarebytes, which uncovered a spate of spam email that name-checks Russian hacking efforts. The subject line for the messages is "Microsoft account unusual sign-in activity." The body reads:

Unusual sign-in activity

We detected something unusual about a recent sign-in to the Microsoft account

Sign-in details

Country/region: Russia/Moscow
IP address:
Date: Sat, 26 Feb 2022 02:31:23 +0100
Platform: Kali Linux
Browser: Firefox
A user from Russia/Moscow just logged into your account from a new device, If this wasn't you, please report the user. If this was you, we'll trust similar activity in the future.

Report the user

Thanks,

The Microsoft account team

The emails then provide a button to "report the user," and an unsubscribe option. Clicking the button creates a new message with the to-the-point subject line of "Report the user." The recipient's email address references Microsoft account protection.

"People sending a reply will almost certainly receive a request for login details, and possibly payment information, most likely via a bogus phishing page." "It's also entirely possible the scammers will keep everything exclusively to communication via email. Either way, people are at risk from losing control of their account to the phishers. The best thing to do is not reply, and delete the email."

As ever, the spam offers up red flags in the form of grammatical errors, including misspellings, such as "acount." In other words, it's not a particularly sophisticated effort, but it's a savvy one. As is the case with any major world event, cresting interest (or fear) is catnip for social engineers.

"Given current world events, seeing 'unusual sign-in activity from Russia' is going to make most people do a double, and it's perfect spam bait material for that very reason," researchers said. "[The emails] (deliberately or not) could get people thinking about the current international crisis. Being on your guard will pay dividends over the coming days and weeks, as more is sure to follow."

The mail explicitly targets Microsoft account holders, but the good news is that Outlook is sending the emails directly to the spam folder, according to Malwarebytes. However, the firm pointed out that, "depending on personal circumstance and/or what's happening in the world at any given moment, one person's 'big deal' is another one's 'oh no, my stuff.'

That's all it may take for some folks to lose their login, and this mail is perhaps more salient than most for the time being."

Source: https://threatpost.com/

Our CEO Is A Published Author

Stay one step ahead of cyber criminals to protect your business, your customers, and your money!

In Jason's first published book, he talks about why cybercrime today cannot be ignored and why your network and data are cyber criminals' #1 target!

Learn all the ways to protect yourself and your data. Contact us today for your copy of *Inside The Hacker Mind.*

Meet Matt Smith

Meet Matt Smith!

Matt is our newest technician at Preferred IT Group. He is CompTIA certified and finishing his bachelor degree in Cybersecurity with Western Governor's University

Matt enjoys gaming, exercising, and playing with his cat Leo.

Welcome to the team!

Grabbing The Bull By The Hornes - Preferred IT CEO, Jason Horne, Is Gaining Ground Fast

Check out Preferred IT Group's CEO, Jason Horne in MSP Success Magazine!

"So, in the sports bar that night, where patrons sampled cold beer and cheered on the Cubs and Komets, a vision for what would become Preferred IT emerged."

MSP SUCCESS
MAGAZINE
Grabbing The Bull By The Hornes
Preferred IT CEO, Jason Horne, Is Gaining Ground FAST
Page 14
Marcus Lemonis Reveals
Now Is The Time To Double Down On Marketing
Page 22
LANDING YOUR MOON SHOT
Buzz Aldrin Talks About Hitting BIG Goals
Page 8
Determination That Won't Quit
Shark Tank's Barbara Corcoran's Rise To New York Realty Royalty: How You Can Dominate Sales Like The Queen
Page 17
MSP SUCCESS
Special Edition: Winter 2022
MSPSuccessMagazine.com
Jason Horne, Co-Founder Of Preferred IT Group

FUN FACT!

Email is the primary entry point of 94% of malware attacks

preferred IT group

preferred IT group

CONTACT US

Fort Wayne	Warsaw
260.440.7377	**574.306.4288**
Columbia City	**Indianapolis**
260.213.4266	**317.426.8180**

www.preferreditgroup.com

6333 Constitution Drive
Fort Wayne, IN 46804

Subscribe to our blog and follow us on social media.